(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－354048
（P2002－354048A）
(43)公開日　平成14年12月6日(2002.12.6)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
H04L	12/66		H04L	12/66	A	5K030
	12/46			12/46	A	5K033
					E	
	12/56	100		12/56	100Z	

審査請求　未請求　請求項の数5　ＯＬ　（全７頁）

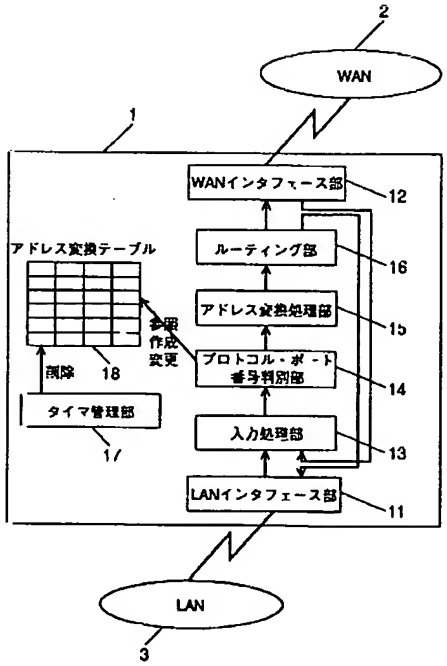
(21)出願番号　特願2001－160311(P2001－160311)
(22)出願日　平成13年５月29日(2001.5.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　村川　泰
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　原口　雅彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　ルータ装置

(57)【要約】
【課題】　適切な通信接続性を確保し、効率的にメモリを利用可能としたルータ装置の提供を目的とする。
【解決手段】　ＷＡＮ２とＬＡＮ３との間に介在してアドレス変換を行うルータ装置１において、一連の通信セッションを識別するプロトコル・ポート番号判別部１４を備え、プロトコル・ポート番号判別部１４は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるものとすることで、アドレス変換機能のために通信セッションが不正に切断されることを防ぎ、適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。



【特許請求の範囲】
【請求項１】グローバルアドレスネットワークとプライベートアドレスネットワークの間に介在してアドレス変換を行うルータ装置において、一連の通信セッションを識別するプロトコル・ポート番号判別部を備え、同プロトコル・ポート番号判別部は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるものであることを特徴とするルータ装置。
【請求項２】前記プロトコル・ポート番号判別部は、前記一連の通信セッションと識別された複数のアドレス変換エントリをグループ化し、グループ毎で一括した操作を行うものであることを特徴とする請求項１記載のルータ装置。
【請求項３】前記プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信プロトコルの性質に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項１記載のルータ装置。
【請求項４】前記プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信相手先に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項１記載のルータ装置。
【請求項５】前記プロトコル・ポート番号判別部は、前記一連の通信セッションを監視し、端末間の通信状態を把握しながらエントリ生存時間を動的に変化させるものであることを特徴とする請求項１記載のルータ装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、グローバルアドレスネットワークとプライベートアドレスネットワークとの間に介在してアドレス変換を行うルータ装置に関し、より詳しくは、ルータ装置におけるアドレス変換エントリ管理方式に関する。
【０００２】
【従来の技術】近年、インターネットの爆発的普及に伴い、小規模なオフィス環境や家庭でも複数台のパーソナルコンピュータ（以下、「ＰＣ」と称す）などの端末をインターネットに接続する需要が高まっている。インターネットへの接続は、ローカルエリアネットワーク（以下、「ＬＡＮ」と称す）を構築し、このＬＡＮに接続されたルータ装置を介して行うのが一般的である。
【０００３】インターネットに接続するにはグローバルＩＰアドレスが必要となるが、これをＬＡＮ内の端末の台数分確保するのは非常に困難なので、通常ＬＡＮ内ではプライベートＩＰアドレスを用いる。そして、インターネットを介して通信をする場合、ルータ装置上でＮＡＴ（Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）やＩＰマスカレードと呼ばれるアドレス変換を行うことでインターネットへ接続する。
【０００４】以下、従来のアドレス変換方式について説明する。
【０００５】図８は従来のネットワーク構成とアドレス変換処理の概要を示す図である。
【０００６】図８において、ＰＣ１０１，１０２，１０３はＬＡＮ１０４に接続されている。ルータ装置１０５はＬＡＮ１０４とインターネット１０６との間に介在し、これらの間でアドレス変換を行う。また、インターネット１０６には端末１０７が接続されているものとする。なお、ＰＣ１０１のＩＰアドレスをＡ、ルータ装置１０５のインターネット１０６側のＩＰアドレスをＢ、端末１０７のＩＰアドレスをＣとする。
【０００７】ＰＣ１０１から端末１０７にパケットを送信する場合、送信元ＩＰアドレスはＡ、宛先ＩＰアドレスはＣのパケットとなる。このパケットは、ルータ装置１０５によりインターネット１０６に向けてルーティングされるが、アドレス変換機能により送信元ＩＰアドレスＡがルータ装置１０５のインターネット１０６側のＩＰアドレスであるＢに書き換えられる。このとき、ルータ装置１０５のアドレス変換テーブルには、この変換に関するアドレス変換エントリが追加され、以後、ＰＣ１０１と端末１０７の間で行われる同じプロトコルの通信に関してはこのアドレス変換エントリが参照されアドレス変換が行われる。また、ルータ装置１０５のメモリには容量の上限があるため、一定時間の参照のないアドレス変換エントリはテーブルから削除される。このアドレス変換機能により、プライベートアドレスで構築されるＬＡＮ１０４内の端末からインターネット１０６に接続することが可能になる。
【０００８】
【発明が解決しようとする課題】しかしながら、上記従来の方式では、ルータ装置１０５はＬＡＮ１０４内からの接続のたびにアドレス変換エントリを生成し、このエントリが決めた規則に則ってアドレス変換を行うだけであり、各アドレス変換エントリ間の関係性を考慮していない。このため、アドレス変換テーブルのメモリ利用が効率的でなく、テーブル中のアドレス変換エントリの数が増えるにつれてエントリ検索に時間が掛かることになる。その結果、通信セッションが終了していないにも関わらず、エントリの生存時間切れと判定されて不当に通信セッションが切断されることも起こりうる。
【０００９】ここで、図９を用いて上記従来の方式によるアドレス変換処理によって起こりうる問題について詳細に説明する。図９において、１１１はプライベートアドレスネットワーク内のＰＣ、１１２はルータ装置、１１３はグローバルアドレスネットワーク内の端末である。ここでは、ＰＣ１１１がＦＴＰクライアント、端末１１３がＦＴＰサーバとなってＦＴＰ通信を行う場合を考える。なお、ＰＣ１１１，ルータ装置１１２，端末１１３のＩＰアドレスをそれぞれＡ，Ｂ，Ｃとする。
【００１０】ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐ

rotocol）は、FTP通信の制御命令のやりとりをするFTP制御コネクション（TCPポート21番）と、実際にデータ転送を行うFTPデータコネクション（TCPポート20番）という2つのコネクションによりFTP通信を行う。PC111から端末113に対してFTP通信を行う場合、ルータ装置112がこれらの間に介在してアドレス変換を行う。ルータ装置112は、PC111からのパケットについては送信元IPアドレスをAからBに変換してから端末113に転送し、端末113からのパケットについては宛先IPアドレスをBからAに変換してPC111に転送する。

【0011】ここで、PC111が端末113から巨大なファイルをダウンロードする場合、FTPデータコネクションにおいてファイル転送をしている間、FTP制御コネクションの方には通信が発生しないため、このコネクションに関するルータ装置112内のアドレス変換エントリの生存時間が切れ、エントリが削除されてしまう。したがって、データ転送終了後にPC111から端末113にFTP制御命令を送ろうとしても、ルータ装置112は既にそれに対応したアドレス変換エントリを削除しているため新規にエントリを作成しなければならず、端末113において別セッションとみなされてパケット破棄され、FTP通信が正常に完遂できなくなる。

【0012】そこで、本発明では、適切な通信接続性を確保し、効率的にメモリを利用可能としたルータ装置を提供することを目的とする。

【0013】

【課題を解決するための手段】上記課題を解決するための本発明のルータ装置は、ルータ装置を通過する通信を監視し、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるように構成したものである。

【0014】本発明のルータ装置によれば、適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。

【0015】

【発明の実施の形態】請求項1に記載の発明は、グローバルアドレスネットワークとプライベートアドレスネットワークの間に介在してアドレス変換を行うルータ装置において、一連の通信セッションを識別するプロトコル・ポート番号判別部を備え、同プロトコル・ポート番号判別部は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるものであることを特徴とするルータ装置であり、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことができる。

【0016】請求項2に記載の発明は、プロトコル・ポート番号判別部は、一連の通信セッションと識別された複数のアドレス変換エントリをグループ化し、グループ毎で一括した操作を行うものであることを特徴とする請求項1記載のルータ装置であり、アドレス変換テーブルにおけるメモリ利用を効率化し、グループ毎で一括した操作を行うことで、エントリ管理の簡易化、高速化が可能となる。

【0017】請求項3に記載の発明は、プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に通信プロトコルの性質に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置であり、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことができ、効率的なメモリ利用が可能となる。

【0018】請求項4に記載の発明は、プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信相手先に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置であり、アドレス変換機能の安全性を高めることができる。

【0019】請求項5に記載の発明は、プロトコル・ポート番号判別部は、一連の通信セッションを監視し、端末間の通信状態を把握しながらエントリ生存時間を動的に変化させるものであることを特徴とする請求項1記載のルータ装置であり、効率的なメモリ利用が可能となる。

【0020】以下、本発明の実施の形態について、図面を参照しながら説明する。

【0021】（実施の形態1）図1は本発明の第1実施の形態におけるネットワーク構成を示す図である。第1実施の形態と従来の技術との相違点は、アドレス変換エントリを関連付け、その生存時間の同期を行うところにある。

【0022】図1において、本発明の第1実施の形態におけるルータ装置1は、グローバルアドレスネットワークとしてのインターネットなどのワイドエリアネットワーク（以下、「WAN」と称す）2と、プライベートアドレスネットワークとしてのLAN3との間に介在してアドレス変換を行うものである。ルータ装置1は、LAN3に接続するLANインタフェース部11、WAN2に接続するWANインタフェース部12、入力したIPパケットが本ルータ装置1により処理すべきものかどうか識別する入力処理部13、処理するパケットの内容の詳細を監視しアドレス変換テーブル18のエントリの参照、追加および内容変更を行うプロトコル・ポート番号判別部14、実際にパケットのアドレス変換を行うアドレス変換処理部15、パケットの適切なインタフェースへの転送を行うルーティング部16、アドレス変換テーブル18を監視し、一定時間参照のないエントリを削除するタイマ管理部17により構成される。アドレス変換テーブル18は、ルータ装置1のメモリ内部に確保され、アドレス変換処理の内容を記述したエントリを集積したものである。

【００２３】ここで、図２を用いて従来のアドレス変換テーブルのエントリの構造と本実施の形態におけるアドレス変換テーブル１８のエントリの構造の相違について説明する。図２（ａ）は従来のアドレス変換テーブルの構造であるが、アドレス変換処理に必要な情報がすべて含まれるエントリが新規の通信コネクションが生じる毎に生成される。図２（ｂ）は本実施の形態におけるアドレス変換テーブル１８の構造であるが、エントリがパケットの送信元、宛先部分（ＩＰレベル）と、その上位のプロトコルに関する部分（上位層レベル）とに階層化されている。また、この中で複数のエントリによって１つの通信セッションを構成するエントリが関連付けられている。

【００２４】図３は本実施の形態のルータ装置１によるアドレス変換処理の流れを示すフローチャート、図４は本実施の形態のルータ装置１によるアドレス変換エントリのグループ化とエントリの生存時間の同期についての説明図である。

【００２５】図４において、３ａはＬＡＮ３に接続されたＰＣ、２ａはＷＡＮ２上の端末であり、ＰＣ３ａ、ルータ装置１、端末２ａのＩＰアドレスをそれぞれＡ、Ｂ、Ｃとする。ＰＣ３ａから端末２ａに通信をする度に、図３に示す手順によってルータ装置１のアドレス変換テーブル１８にエントリが追加されるが、エントリ新規作成のたびに図１のプロトコル・ポート番号判別部１４が既存のアドレス変換エントリと関連付けられるものかどうか判定し、図４に示すアドレス変換テーブル１８のようにＦＴＰ制御コネクション（ＴＣＰ２１番）とＦＴＰデータコネクション（ＴＣＰ２０番）エントリが関連付けられる。関連付けられたエントリの生存時間は同期されるため、従来の技術の図９において説明したようなＦＴＰ通信のアドレス変換エントリの不正削除を防ぐことができる。

【００２６】（実施の形態２）以下、本発明の第２実施の形態について、図５を参照しながら説明する。第２実施の形態のルータ装置１におけるアドレス変換処理の概要は、図１～図３で示したところと同様なので説明を省略する。第２実施の形態と従来の技術との相違点は、アドレス変換エントリのグループ化を行い、生存時間の同期などの管理を一括で行うところにある。

【００２７】図５は第２実施の形態におけるルータ装置１のアドレス変換テーブル１８の構成を示す図である。ルータ装置１をパケットが通過する際、図１のプロトコル・ポート番号判別部１４によりパケットは検査され、上位プロトコル、宛先ポート番号などから、図５に示すようにエントリはグループ化され、エントリ中の生存時間はグループ内のエントリで統一され、生存時間管理などの処理が一括化される。

【００２８】（実施の形態３）以下、本発明の第３実施の形態について、図６を参照しながら説明する。第３実施の形態のルータ装置１におけるアドレス変換処理の概要は、図１～図３で示したところと同様なので説明を省略する。第３実施の形態と従来の技術との相違点は、通信プロトコルの種別、状態によってアドレス変換エントリ生存時間を最適化するところにある。

【００２９】図６は第３実施の形態におけるルータ装置１によるアドレス変換エントリの生存時間の設定例を示す図である。例えば、ＩＰの上位層のプロトコルについて、通信持続性が低い順番に、ＩＣＭＰ、ＵＤＰ、ＴＣＰの順に生存時間の値を上げていく。また、その中でもコネクション型通信プロトコルであるＴＣＰについては、その上で利用されるプロトコルによって、ＴｅｌｎｅｔやＦＴＰなどの通信の持続性が高いプロトコルと、ＰＯＰ３といった通信の持続性が低いプロトコルとでアドレス変換エントリ新規作成時にアドレス変換エントリ生存時間に高低をつける。

【００３０】（実施の形態４）以下、本発明の第４実施の形態について、図７を参照しながら説明する。

【００３１】図７は第４実施の形態におけるネットワーク構成を示す図である。第４実施の形態のルータ装置１におけるアドレス変換処理の概要は、図１～図３で示したところと同様なので説明を省略する。第４実施の形態と従来の技術との相違点は、接続先のネットワーク毎にアドレス変換エントリ生存時間を変更することにある。

【００３２】図７において、２ｂはインターネット、２ｃ，２ｄはＰＣ３ａの通信先となるネットワークである。ルータ装置１に予め信頼性の高いネットワークのＩＰアドレスを指定できるようにする。ネットワーク２ｃは登録されたネットワークである。ＰＣ３ａから外部ネットワークに通信を行う場合、ルータ装置１にアドレス変換エントリが生成されるが、それがルータ装置１に登録済のネットワーク２ｃである場合、他の相手先に接続した場合よりも長いエントリ生存時間を設定する。こうすることで、家庭内ネットワークから勤務先のネットワークにＴｅｌｎｅｔした場合などで、常に相手先と通信をしていなくても、アドレス変換エントリが削除される心配をする必要がなくなり、未知のネットワークに接続する場合にはエントリ生存時間を短くすることで、その相手先からの不正アクセスをされる危険性を減らすことができる。

【００３３】（実施の形態５）第５実施の形態のルータ装置１におけるアドレス変換処理の概要は、図１～図３で示したところと同様なので説明を省略する。第５実施の形態と従来の技術との相違点は、通信プロトコル状態遷移に同期してアドレス変換エントリ生存時間を最適化するところにある。

【００３４】ルータ装置１内のアドレス変換テーブル１８のエントリを図１のプロトコル・ポート番号判別部１４が参照する場合、上位プロトコルがＴＣＰのパケットについては、ＴＣＰの通信内容を監視し、ＦＩＮメッセ

ージが通過する場合は、該当するエントリの生存時間を短くし、ＲＳＴメッセージが通過する場合には、該当するエントリを削除するといったＴＣＰの状態遷移に応じたエントリ生存時間管理を行う。

【００３５】

【発明の効果】本発明によれば、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことで適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施の形態におけるネットワーク構成を示す図

【図２】（ａ）従来のアドレス変換テーブルの構造を示す図

（ｂ）本実施の形態におけるアドレス変換テーブルの構造を示す図

【図３】本実施の形態のルータ装置によるアドレス変換処理の流れを示すフローチャート

【図４】本実施の形態のルータ装置によるアドレス変換エントリのグループ化とエントリの生存時間の同期についての説明図

【図５】第２実施の形態におけるルータ装置のアドレス変換テーブルの構成を示す図

【図６】第３実施の形態におけるルータ装置１によるアドレス変換エントリの生存時間の設定例を示す図

【図７】第４実施の形態におけるネットワーク構成を示す図

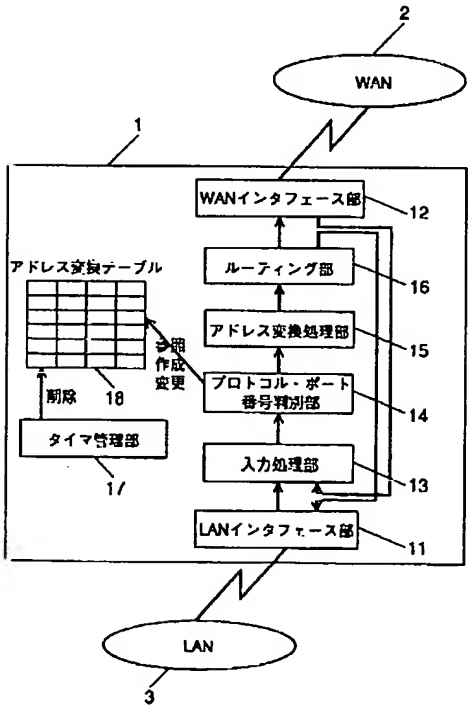
【図８】従来のネットワーク構成とアドレス変換処理の概要を示す図

【図９】従来の方式によるアドレス変換処理によって起こりうる問題点を示す説明図

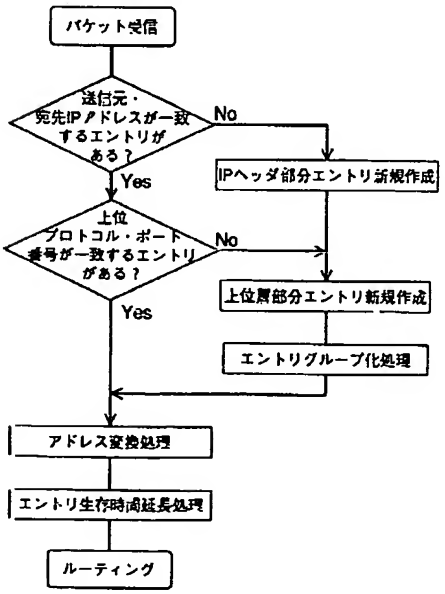
【符号の説明】

１　ルータ装置
２　ＷＡＮ
２ａ　端末
２ｂ　インターネット
２ｃ，２ｄ　ネットワーク
３　ＬＡＮ
３ａ　ＰＣ
１１　ＬＡＮインタフェース部
１２　ＷＡＮインタフェース部
１３　入力処理部
１４　プロトコル・ポート番号判別部
１５　アドレス変換処理部
１６　ルーティング部
１７　タイマ管理部
１８　アドレス変換テーブル

【図１】

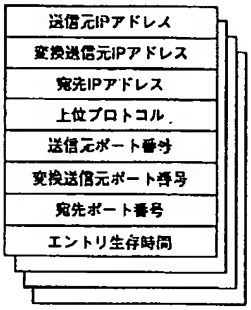


【図３】

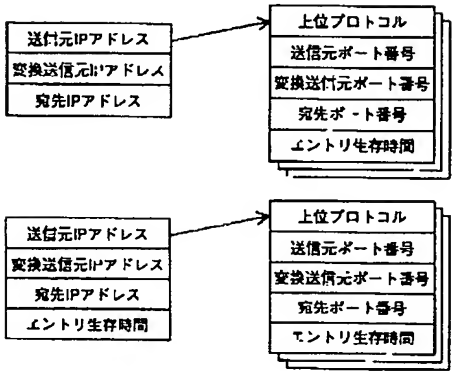


【図2】

(a)



(b)



【図4】

ルータ装置1のアドレス変換テーブル18

送信元=A	プロトコル	送信元	宛先	生存時間	
変更後=B	TCP	4000	20	300	関連付け
宛先=C	TCP	4001	21	300	

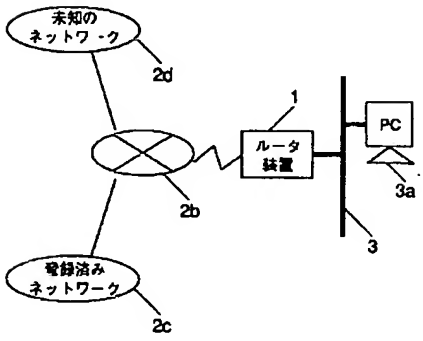
【図6】

上位プロトコル	ポート番号	生存時間
ICMP	—	30秒
UDP	—	5分
TCP	110 (POP3)	10分
	25 (SMTP)	
	⋮	⋮
	21 (FTP)	20分
	20 (FTP)	
	23 (Telnet)	30分

【図5】

送信元IPアドレス / 変更後IPアドレス / 宛先IPアドレス	プロトコル	送信元	宛先	生存時間	
	TCP	4000	20	300	FTPグループ
	TCP	4001	21		
	TCP	4002	80	60	HTTPグループ
	TCP	4003	80		
	TCP	4004	80		
	ICMP	—	—	15	
	UDP	4010	161	150	SNMPグループ
	UDP	4011	162		

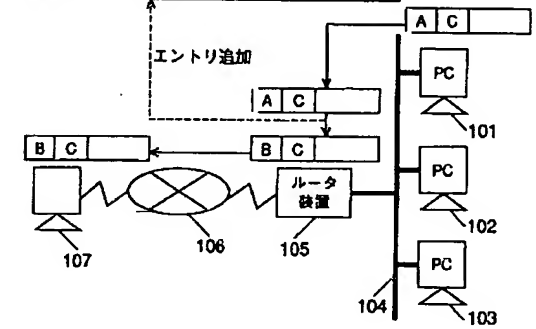
【図7】



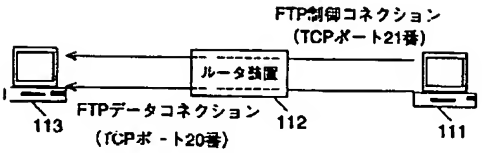
【図8】

ルータ装置105のアドレス変換テーブル

送信元	変更後	宛先	プロトコル	宛先ポート
D	B	X	TCP	80
E	B	Y	UDP	2400
A	B	C	TCP	21



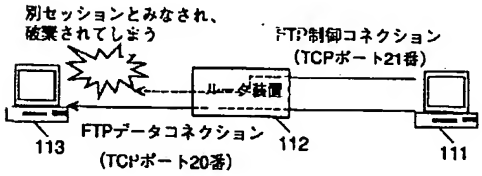
【図9】



ルータ装置112のアドレス変換テーブル

送信元	変更後	宛先	プロトコル	宛先ポート
A	B	C	TCP	21
A	B	C	TCP	20

データコネクションでのデータ転送が続くうち、FTP制御コネクションに関するエントリが削除



ルータ装置112のアドレス変換テーブル

削除

送信元	変更後	宛先	プロトコル	宛先ポート
~~A~~	~~B~~	~~C~~	~~TCP~~	~~21~~
A	B	C	TCP	20

フロントページの続き

Fターム(参考) 5K030 HC01 HC14 HD03 HD06 HD09
KA05 LB05
5K033 CB09 DA06 DB18 EC04